https://doi.org/10.1007/s12083-019-00785-5

PSE-AKA: Performance and security enhanced authentication key agreement protocol for IoT enabled LTE/LTE-A networks

Balu L. Parne[1] · Shubham Gupta[2] · Narendra S. Chaudhari[3]

Received: 23 August 2018 / Accepted: 3 July 2019 / Published online: 13 July 2019

Abstract

In the mobile telecommunication network, Long term Evolution (LTE) is the most successful technological development for the industrial services and applications. The Evolved Packet System based Authentication and Key Agreement (EPS-AKA) was the first protocol proposed to authenticate the communication entities in the LTE network. But, the EPS-AKA protocol suffers from the single key exposure problem and is susceptible to various security attacks. Also, the protocol incurs high bandwidth consumption and computation overhead over the communication network. Moreover, the protocol doesn't support the Internet of Things (IoT) based applications and has several security issues such as the privacy violation of the user identity and key set identifier (KSI). To resolve the above problems, various AKA protocols were proposed by the researchers. Unfortunately, none of the protocols succeeded to overcome the privacy preservation and single key exposure problem from the communication network. In this paper, we propose the performance and security enhanced (PSE-AKA) protocol for IoT enabled LTE/LTE-A network. The proposed protocol follows the cocktail therapy to generate the authentication vectors that improves the performance in terms of computation and communication overhead. The protocol preserves the privacy of objects, protects the KSI and avoids the identified attacks from the communication network. The formal verification and security analysis of the proposed protocol is carried out using the BAN logic and AVISPA tool respectively. The security analysis shows that the protocol achieves the security goals and secure against various known attacks. Finally, the performance analysis shows that the proposed protocol generates the less overhead and reduces the bandwidth consumption from the network.

Keywords LTE/LTE-A · Authentication · IoT · Privacy preservation · AVISPA · KFS/KBS

1 Introduction

The Long Term Evolution Advanced (LTE-A) a.k.a. fourth generation (4G) technology is the recent advancement of third generation (3G) in the mobile communication network. With the development of the mobile application and advanced innovation in the wireless communication, the LTE technology has achieved a phenomenal growth in the wireless telecommunication network. The Internet of Things (IoT) is one of the most promising technology where billions of devices are connected by forthcoming wired and wireless telecommunication network to control and manage various applications in the environment [1–3]. It has a number of applications in various fields such as personal health care monitoring system, smart transportation, smart cities, smart electricity grids, intelligent tracing, and tracking system [4–6]. In an IoT, a unique identifier is assigned to each object to execute certain applications. To support these applications, the objective of the telecommunication network is to provide ubiquitous connectivity among the people as well as the objects/devices [7]. The LTE-advanced (LTE-A) is designed by third generation partnership project (3GPP) with several objectives that enable 4G network with high resource capacity, low latency, flexible bandwidth, higher data rate and good quality of services [8, 9]. Recently, Device to Device (D2D) communication has been evolved in the LTE/LTE-A network [10–12]. Hence, LTE/LTE-A can serve as the best suitable platform for the IoT enabled communication network.

Recently, 3GPP community has started to research the characteristics of IoT objects during communication in the LTE/LTE-A network. There are certain security issues with

✉ Balu L. Parne
balu.parne@vitap.ac.in

Extended author information available on the last page of the article.

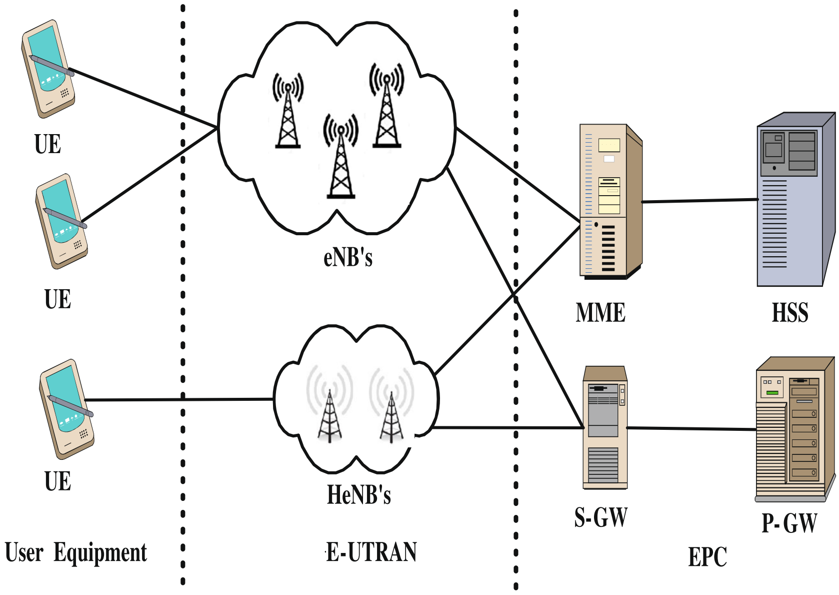


Fig. 1 LTE/LTE-A network architecture

the existing LTE-AKA protocol. Some of the vulnerabilities of the 4G network have been addressed and identified in the [13] and [14]. To establish the secure communication and privacy preservation between objects and server are the main research challenges in an IoT enabled network as there are numerous devices communicate across the networks. To achieve authentication, objects follow the evolved packet system based authentication and key agreement (EPS-AKA) protocol for the LTE/LTE-A network. But, the protocol fails to fulfill the necessary security demands such as user privacy preservation and key forward/backward secrecy (KFS/KBS). Moreover, the protocol suffers from the single key exposure problem and fails to avoid the Denial of Service (DoS), redirection and Man in the Middle (MitM) attack [15]. In addition, the protocol generates the high computation overhead and bandwidth consumption among the communication entities. However, in IoT enabled LTE/LTE-A network the mobile phone and smart meters are the embedded devices that have limited computing resources. Hence, there is need to revisit the EPS-AKA protocol to support the IoT devices for maintaining the information security.

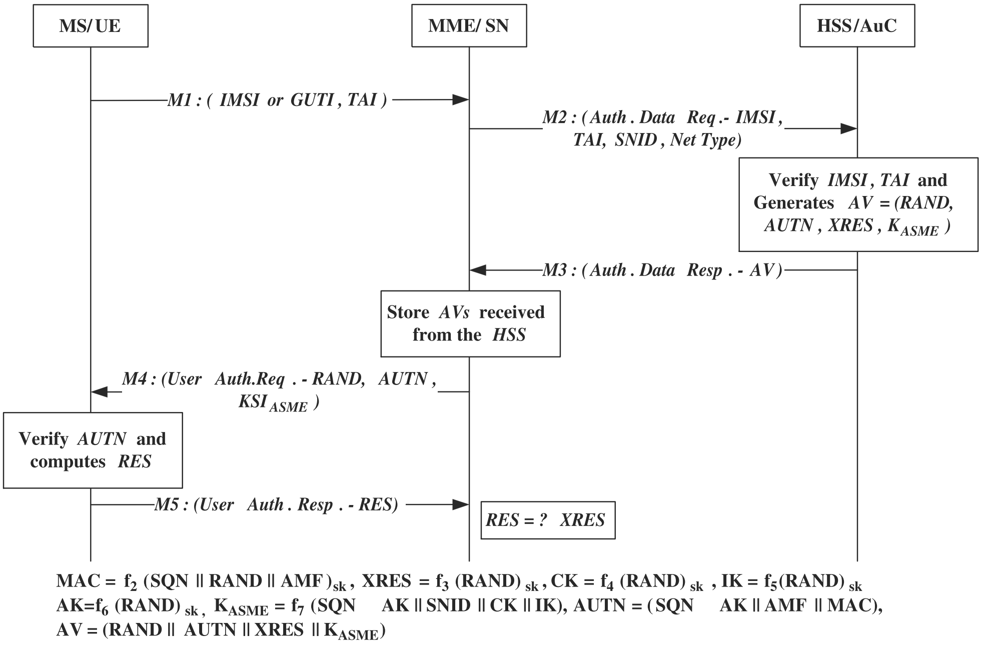
1.1 Existing AKA protocol for LTE/LTE-A network

The LTE/LTE-A network architecture consists of two evolved subsystems: Evolved Packet Core (EPC) and Evolved UTRAN (E-UTRAN) as shown in the Fig. 1. The E-UTRAN has set of base-stations, known as eNodeB, connected to the user equipment/mobile nodes via radio interfaces. These base-stations forward the traffic to EPC with radio resources. The EPC contains the following network entities:

– Mobility Management Entity (MME): This the main control node in the LTE/LTE-A network architecture that manages various security functionalities. Mainly, the MME communicates with the HSS for the authentication of the user equipment/ mobile nodes.
– Serving Gateway (S-GW): The S-GW manages the mobility of users between the P-GW and eNodeB.
– Packet Data Network Gateway (PGW): It is the entity of the EPC that handles the packets of outer networks in order to transfer the traffic of user equipment/mobile nodes.
– Home Subscriber Server (HSS): The database that has information about location and subscription of the user equipment. In addition, it consists of the authentication parameters for the user equipment/ mobile nodes.

To overcome the problem of key secrecy and security attacks in the cellular network, 3GPP proposed the EPS-AKA protocol for the LTE/LTE-A network [16–19]. The authentication is achieved through the challenge-response scheme between the User Equipment (UE) and Mobile Management Entity (MME) in the EPS-AKA protocol as shown in the Fig. 2. The EPS-AKA protocol executes the authentication steps as i) UE requests for the authentication through MME and HSS (Home Subscriber Server) transmits the authentication vectors (AVs) to the MME. ii) Further, the MME selects one of the AV for mutual authentication with MS and both generate the key for access security management entity (K_{ASME}). iii) Once the mutual authentication is achieved, the shared secret keys are generated between the MME and MS

Fig. 2 EPS-AKA protocol for LTE/LTE-A network


MS/ UE
MME/ SN
HSS/AuC
M1 : (IMSI or GUTI , TAI)
M2 : (Auth . Data Req .- IMSI , TAI, SNID , Net Type)
Verify IMSI , TAI and Generates AV = (RAND, AUTN , XRES , K_ASME)
M3 : (Auth . Data Resp . - AV)
Store AVs received from the HSS
M4 : (User Auth.Req . - RAND, AUTN , KSI_ASME)
Verify AUTN and computes RES
M5 : (User Auth . Resp . - RES)
RES = ? XRES
MAC = f2 (SQN || RAND || AMF)sk , XRES = f3 (RAND) sk , CK = f4 (RAND) sk , IK = f5(RAND) sk
AK=f6 (RAND) sk , KASME = f7 (SQN AK || SNID || CK || IK), AUTN = (SQN AK || AMF || MAC),
AV = (RAND || AUTN || XRES || KASME)

for signalling data protection. The EPS-AKA protocol provides the mutual authentication similar to the Universal Mobile Telecommunication System (UMTS) AKA but, the key derivation is different in the protocol. The protocol generates the K_{ASME} instead of cipher key (CK) and integrity key (IK) for secure data transmission.

1.2 Drawbacks of the existing AKA protocol for LTE/LTE-A network

The EPS-AKA protocol fulfils most of the security requirements and protects the communication interface against possible attacks on the network. However, the protocol is still vulnerable to various security attacks and faces critical challenges for IoT enabled services over the communication network.

- In the LTE network, the identity of the user (device) and the key set identifier of access security management entity (KSI_{ASME}) are transmitted in a clear text over the communication channel. An adversary can misuse these parameters to violate the privacy of user identity and keys in the communication network.
- The security of the EPS-AKA protocol depends on the preshared secret key between MS and HSS. Once this key is compromised, all the keys can be retrieved and there is a possibility that an adversary can be authenticated by the network. Moreover, the protocol fails to maintain the KFS/KBS.
- In the EPS-AKA protocol, the UE and HSS maintain the sequence number (SQN) between them. Hence, the protocol suffers from the synchronization conflict.
- The computational complexity of the HSS is very high as all the authentication vectors are generated by the HSS and transmitted to the MME. It incurs the high bandwidth consumption between HSS and MME in the network.
- The protocol doesn't suit to the IoT based services as it violates the privacy of user identity and the KSI_{ASME} over the communication network.

1.3 Security analysis of existing EPS-AKA protocol

In LTE/LTE-A network, there is a possibility of various internal and external attacks from the mobile nodes. The internal attacks can be executed by two sources such as: core network and access network, whereas the external attacks can be performed by adversaries. The EPS-AKA protocol is vulnerable to various security attacks such as redirection, impersonation, MitM, and DoS attack.

1. **Internal Attacks:**
    - The base-stations in LTE/LTE-A network may generate the security vulnerabilities as various eNBs are managed by the same MME. An adversary builds its false base-station and impersonates a legitimate base-station by making the network susceptible to security weaknesses.

- The IP-based architecture of LTE/LTE-A network has made it vulnerable to security risks such as eavesdropping attacks as compared to the UMTS networks. In addition, the LTE/LTE-A network suffers from the malicious attacks such as internet worms, spams, etc.

2. **External Attacks:**

- Privacy preservations and Protection: The EPS-AKA protocol fails to provide privacy preservation and protection. Whenever the user registers to the network, MME sends the request of the IMSI to the user and the user sends the IMSI over the communication channel without any encryption. Once the users identity is disclosed, it may suffer from several security attacks.
- Key Forward/Backward Secrecy: The LTE key mechanism follows the chaining architecture in which the eNB computes the new keys from the current key with other parameters. Once the current eNB is tempered, then the successive keys can be compromised very easily. Hence the KFS/KBS is not achieved in the EPS-AKA protocol.
- Redirection Attack: In the EPS-AKA protocol, the mutual authentication among the communication entities is not carried out. Hence, an adversary may place the bogus eNB that performs as a legitimate one and broadcasts the authentication messages to the MS/UE.
- Impersonation Attack: In this attack, an adversary eavesdrops the signalling messages of the target users. The EPS-AKA protocol fails to preserve the privacy of communication entities. Therefore, the protocol suffers from the impersonation attack as an adversary impersonates as a legitimate entity and transfers the signalling messages to the network in order to believe that it emerges from the authentic user.
- MitM Attack: In the EPS-AKA protocol, authentication among the communication entities is carried out in only one direction. So, there is possibility that an intruder may place in between the authentic entities and impersonate as the legitimate entity. Also, there is possibility of the eavesdropping of the signalling messages.
- DoS Attack: In the protocol, an adversary sends several bogus request messages to the MS and keep the network busy. Also, the protocol follows SQN to authenticate HSS/MS. If an adversary makes a false registration attempt by replying to the UE (message M4 Fig. 1), the SQN becomes inconsistent as the value of SQN increased by one. If the legitimate MS attempts to build the connection, it will never succeed due to MAC failure. Therefore, the MS suffers from the DoS attack.

In future, it is expected that efficient and secure services will be provided by the LTE/LTE-A network to the IoT objects. Moreover, there is a possibility that the IoT devices may increase the network overhead by transferring bogus traffic over the communication channel. This problem will occur when the victim object fails to authenticate the legitimate object connected to the network. Therefore, it is important to revisit the EPS-AKA protocol to provide mutual authentication in the IoT enabled network. The proposed protocol must eliminate all the identified attacks from the communication network. In addition, the protocol should be efficient in terms of communication and computation overhead as compared to the existing LTE/LTE-A protocols.

1.4 Core technical contribution

To avoid all the above mentioned issues, we propose the performance and security enhanced (PSE-AKA) protocol for an IoT enabled LTE/LTE-A network. The main contributions are as follows:

1. The protocol follows the basic architecture of the LTE/LTE-A network recommended by the 3GPP and accommodates all the security requirements of the IoT enabled communication network.
2. The proposed protocol preserves the privacy of object/device identity during the AKA process. Also, the protocol secures the KSI_{ASME} without transmitting it over the communication network.
3. In the proposed protocol, we resolve the single key exposure problem by securing the preshared secret key between the UE and HSS. It maintains the key secrecy and the freshness of the keys used in the authentication process.
4. The protocol follows the cocktail therapy to generate the authentication vectors that reduces the computational overhead and the bandwidth consumption between the communication entities in the network.
5. The formal verification of the proposed protocol is carried out by BAN logic and simulated using Automated Validation of Internet Security Protocol Application (AVISPA) tool for the correctness.
6. The security analysis shows that the protocol accomplishes all the security requirements and eliminates the identified security attacks from the LTE/LTE-A network.
7. The performance analysis of the proposed PSE-AKA protocol has significant improvement in the bandwidth consumption between HSS and MME. In addition, the

protocol incurs the competitive overheads compared to the existing AKA protocols.

1.5 Organization of the paper

The remaining sections of the paper are organized as follows. In Section 3, we review the existing AKA protocols of the LTE/LTE-A network. The proposed PSE-AKA protocol for IoT enabled LTE/LTE-A network is illustrated in Section 3. Section 4 illustrates the formal verification of proposed protocol using BAN logic model and the AVISPA tool. The security analysis of the proposed protocol in terms of the security goals, key privacy properties and resistance against various attacks is carried out in Section 5. The performance analysis of the proposed PSE-AKA protocol with respect to existing AKA protocol is illustrated in Section 6. Finally, Section 7 concludes the paper.

2 Review of authentication protocols in LTE/LTE-A network

There are various AKA protocols proposed by the researchers to improve the authentication efficiency, security, and performance of the LTE/LTE-A networks. The privacy preservation and security against various attacks in the network are the major concerns of the LTE/LTE-A network. Many symmetric and asymmetric key based AKA protocols were proposed to avoid these problems in the LTE/LTE-A network [20–27]. The IoT application based on LTE/LTE-A network is the current focus of the research as it provides the best communication channel for these applications. [4, 28, 29].

A novel 3GPP system architecture evolution (SAE) AKA protocol was proposed by Deng et al. to overcome the problems of existing EPS-AKA protocol [20]. The author analysed the protocol adopted by the 3GPP system and pointed out the security issues in the network. The protocol suffers from lack of mutual authentication that leads to the possibility of traffic redirection from one network to another. Moreover, an adversary may intercept the AVs due to their unsecured transmission. To solve these problems, public key cryptosystem based an improved SAE-AKA protocol was proposed. But, the protocol suffers from the various security issues such as violation of user identity and authentication vectors. Also, the protocol incurs the high computation overhead because of the public key cryptosystem. To overcome the above problems, Vintila et al. introduced the J-PAKE (Authenticated Key Exchange by Juggling) algorithm that maintains the KFS/KBS [18, 30]. However, the scheme fails to preserve the privacy and suffers from the impersonation and DoS attack. Koien proposed an enhanced EPS-AKA (EAKA) protocol to establish the mutual authentication between the communication entities [25]. The protocol follows the conventional challenge-response scheme but, modifies the authentication token in the AVs. However, the protocol does not preserve the privacy of communication entities and suffers from the MitM attack. To reduce the computational consumption from the network, an improved AKA (I-AKA) protocol was proposed by Gu and Gregory [21]. The protocol meets the security requirements defined by the 3GPP and provides security against DoS attack. However, the protocol fails to protect the user identity and susceptible to MitM attack.

Li and Wang proposed the security enhanced AKA protocol based on public key framework [26]. The protocol preserves the user identity and avoids the various known attacks from the network. Due to public key cryptosystem modular exponentiation, the protocol generates the high network overhead during the authentication process. To improve the efficiency of the EPS-AKA protocol in terms of bandwidth consumption and computation overhead, an enhanced AKA protocol is proposed by Purkhiabani and Salahi [17]. The protocol avoids the redirection attack but, is susceptible to identity catching and MitM attack. Further, Choudhury et al. proposed the protocol to resolve the problem of privacy preservation in the LTE/LTE-A network [31]. In the protocol, a dynamic mobile subscriber identity (DMSI) is sent by the UE in place of the IMSI. The DMSI updates its value based on the recently received random number by UE during successful AKA process. However, the protocol incurs high computation overhead to encrypt and decrypt the user identity on the sender and receiver side respectively and vulnerable to various attacks. Prasad and Manoharan proposed digital signature based AKA protocol for LTE/LTE-A network [32]. The protocol incurs low computation as it follows the digital signature based approach. Moreover, there is less delay because of only two message exchanged during the authentications. However, the trusted third party is involved to establish the trust among the communication entities. Hence, if the third party is compromised then the whole communication network will be vulnerable to various known attacks.

Hamandi et al. proposed the hybrid key cryptosystem based privacy enhanced AKA protocol to preserve the privacy of UE in LTE/LTE-A network [23, 33]. The protocol improves the security and preserves the privacy of the communication entities. However, the communication entities use the sequence numbers during the message transmission and suffer from the synchronization problem. Moreover, the protocol generates the high computation overhead as it follows the hybrid key cryptosystem. Ramadan et al. proposed the secure LTE-AKA protocol to avoid the problem of false base station and IMSI catching attack [34]. The protocol generates the high computation overhead due to asymmetric key operations. Baza et al. proposed an efficient distributed approach for key management in micro grids [35]. This is the distributed key management scheme with authentication capability to avoid the single-point failure problem by removing the need for using a meter data management system in the smart grid technology. However, there is single group key shared with all the smart meters and they have not taken care the security of single shared symmetric key among the devices. To preserve the privacy and protect the shared secret key, Degefa et al. proposed the performance and security enhanced AKA protocol [36]. Moreover, Saxena et al. proposed the AKA for an IoT enabled LTE/LTE-A network [37]. These protocols overcome the issues of the EPS-AKA protocol and achieve the efficient communication among the various IoT devices. However, there is high bandwidth consumption between the communication entities (from HSS to MME) in the network to transmit the authentication vectors. Mohammadali et al. proposed a novel identity-based key establishment method for advanced metering infrastructure in smart grid [38]. This is one of the application of the key management in the IoT based infrastructure in the smart grid technology. The protocol employs elliptic curves at its core and has the lowest computational overhead among current secure protocols, especially at the meter side. However, the protocol fails to preserve the privacy of the user identity as well as single shared secret key between the communication entities.

From the literature survey of AKA protocols, it can be observed that most of the existing protocols are vulnerable to various attacks and suffers from high network overhead. In addition, the protocols do not preserve the user identity and KSI_{ASME} over the communication network. Moreover, the symmetric key cryptosystem based protocols suffer from key exposure problem. Once this key is tampered, each key can be negotiated by the adversary. However, it is possible to achieve the secure mutual authentication in LTE/LTE-A network using the public key cryptosystem. The extensive research on AKA protocols in LTE/LTE-A network exploits the problems of public key cryptosystem such as high bandwidth consumption and overhead. In addition, these protocols perform the extensive and time consuming key operations such as bilinear pairing, modular exponentiation and point multiplication that doesn't suit for the resource constrained devices in IoT based applications. Hence, to overcome the above mentioned issues, we propose the symmetric key based PSE-AKA protocol for IoT enabled LTE/LTE-A network. The protocol accomplishes all the security requirements as privacy preservation, data integrity, confidentiality and key secrecy. Moreover, the proposed protocol preserves the privacy of the communication entities and protects the KSI_{ASME} that maintains KFS/KBS. The proposed protocol reduces the computational overhead, avoids the signaling congestion from the network and known attacks during the AKA process.

3 The proposed PSE-AKA protocol

There are several protocols were proposed in the literature to overcome the problems of the EPS-AKA protocol for the LTE/LTE-A networks. The existing protocols follows the symmetric/ asymmetric key cryptosystem. The asymmetric key based protocol generates the high computation overhead so they are not suitable for the resource constrained devices in the IoT enabled communication network [39]. Saxena et al. proposed the symmetric key based AKA protocol for an IoT enabled LTE/LTE-A network [37]. The protocol overcomes the issues of the EPS-AKA and achieves the efficient communication among the IoT enabled devices. However, there is possibility of attack on the symmetric key shared among the communication entities. Once this key is tampered, each key can be negotiated by the adversary. Moreover, there is high bandwidth consumption between the communication entities (from HSS to MME) in the network to transmit the authentication vectors. Hence, the protocols in the literature needs to revise to make them suitable for the IoT enabled devices. In the proposed protocol we have overcomes the mentioned issues and design a symmetric key based PSE-AKA protocol.

This section illustrates the proposed PSE-AKA protocol for the IoT enabled LTE/LTE-A network, which avoids the identified attacks from the existing EPS-AKA protocol. The proposed protocol adopts the cocktail therapy [40] to generate the AV's that reduces the computation overhead of the HSS and minimizes the bandwidth utilization between the communication entities. The proposed protocol strictly follows the framework of the LTE/LTE-A network and avoids the single key exposure problem by protecting the pre-shared secret key. The protocol avoids the various security attacks from the communication network. Additionally, the protocol preserves the privacy of communication entities. The standardized notations and symbols of the proposed protocol are shown in Table 1.

3.1 Basic assumption/Pre-shared parameters:

In the proposed protocol, the following assumptions are made as in conventional cellular networks:

- The secret key K is defined by 3GPP stored at AuC of HSS. The session key SK, generated by K, is used at both ends.
- The AuC at the HSS is a trusted server that does not transmit the messages encrypted by the SK of one UE to the other. Also, it is assumed that the path between

Table 1 Symbols/Abbreviations and definitions

Symbol/Abbreviation	Definition	Size (in bits)
IMSI	International Mobile Subscriber Identity	128
TMSI	Temporary Mobile Subscriber Identity	128
PID/TID	Permanent/Temporary Identity of device	128
GUTI	Global Unique Temporary Identity	128
AMF	Authentication Management Field	48
LAI	Location Area Identity	40
SN_{ID}	Serving Network identity	128
ACC	Accumulator	24
DMSI	Dynamic Mobile Subscriber Identity	128
SQN / $XSQN$	Sequence Number	48
AUTN	Authentication Token	Variable
AUTH/XAUTH	Authentication of individual device	128
AV/GAV/GMAV	Authentication Vector	Variable
MAC/$XMAC$	Message Authentication Code	64
RES/$XRES$	Response/Expected response message	64
$RAND$	Random Number	128
CK/IK/DK/AK	Cipher/Integrity/Delegation/Anonymity Key	128
K / SK	Shared secret key between UE and HSS	128
KID	Key identifier of K_{GRP1-i}	128
$SSDK$	Secure secret dynamic key	128
KSI_{ASME} / $XKSI_{ASME}$	Key Set Identifier of K_{ASME}	3
K_{ASME}	Access Security Management Entity Key	256
MSK	Master Session Key	128
LC	Lagrange Components	128
T/TS	TimeStamp	64
RES/ $XRES$	Response/ Expected Response	64
IV / SV	Initialization Vector/Secret Value	128
XCV / CV	Confirmation Value	256
PN	Prime Number	128
ECDH	Elliptic Curve Diffie Hellman key	192
ECDS	Elliptic Curve Digital Signature key	448

MME and HSS is secure on the basis of diameter protocol [41, 42].

- KID is introduced as a unique key identifier that points to the K. The KID is changed or reallocated after each successful AKA process.
- E/D are newly introduced functions based on the ciphering algorithm that supports the UE and HSS to encrypt/decrypt transmitted messages over the network.
- The proposed protocol uses the various functions to generate authentication parameters. Table 2 defines the role of various cryptographic functions that generate the respective authentication parameters.

3.2 Phase-1: authentication vector distribution phase

This phase is performed when an UE moves into the location area of another MME for the first time. In this phase, the UE requests to access the LTE/LTE-A network by the HSS through MME. The main purpose of the registration phase is to issue the prescriptive AV (PAV) from the HSS to the local MME. Therefore, the MME and UE authenticate to each other (Fig. 3).

Table 2 Cryptographic functions with their roles

Function	Role
$f_1'()$	To generate key SDK
$f_2()$	To generate $MAC/XMAC$
$f_3()$	To generate $RES/XRES$
$f_4()$	To generate key CK
$f_5()$	To generate key IK
$f_6()$	To generate key AK
$KDF()$	To generate key K_{ASME}
$f'()$	To generate key KSI_{ASME}

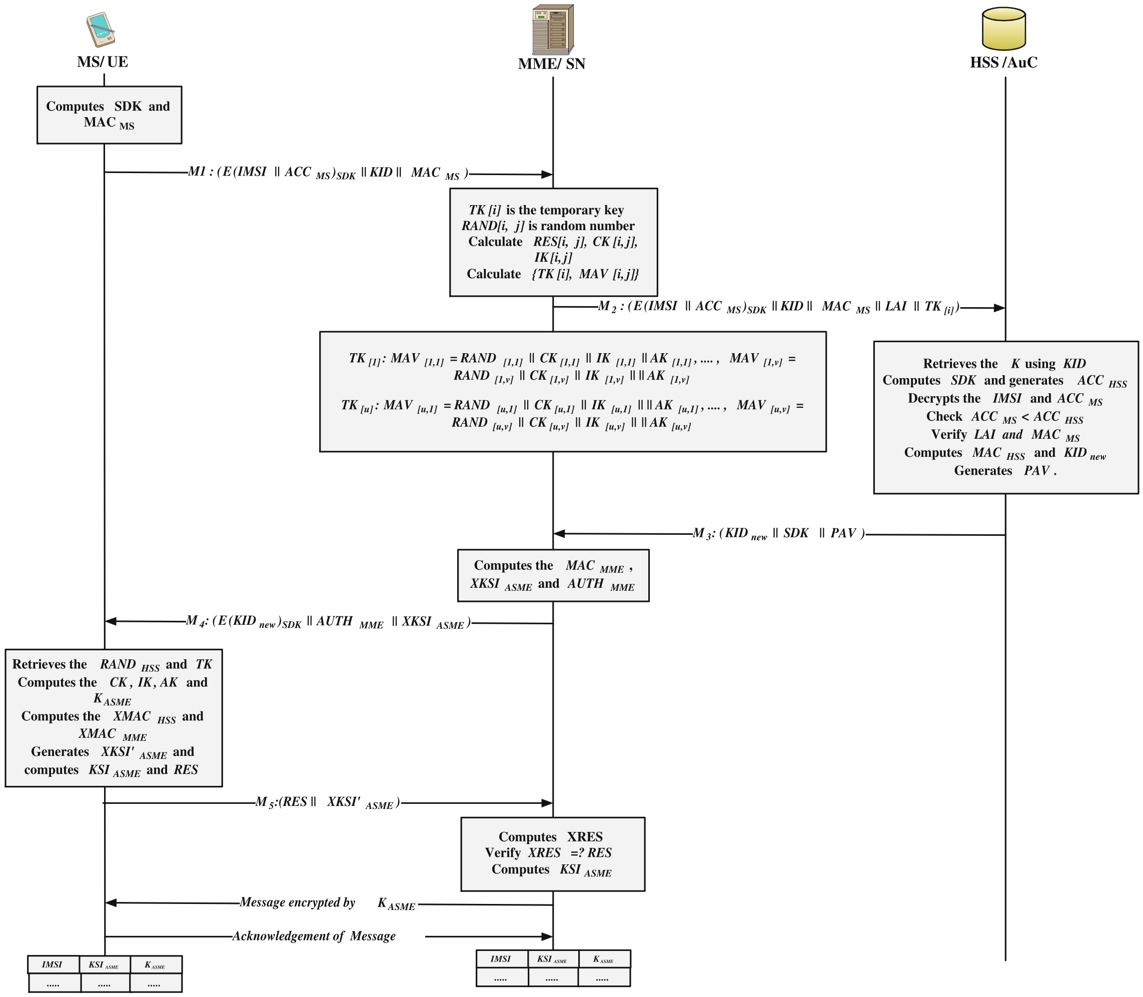

MS/ UE
MME/ SN
HSS /AuC
Computes SDK and MAC_{MS}
$M1 : (E(IMSI \| ACC_{MS})_{SDK} \| KID \| MAC_{MS})$
$TK[i]$ is the temporary key
$RAND[i, j]$ is random number
Calculate $RES[i, j]$, $CK[i,j]$, $IK[i,j]$
Calculate $\{TK[i], MAV[i,j]\}$
$M_2 : (E(IMSI \| ACC_{MS})_{SDK} \| KID \| MAC_{MS} \| LAI \| TK_{[i]})$
$TK_{[1]}: MAV_{[1,1]} = RAND_{[1,1]} \| CK_{[1,1]} \| IK_{[1,1]} \| AK_{[1,1]}, ..., MAV_{[1,v]} = RAND_{[1,v]} \| CK_{[1,v]} \| IK_{[1,v]} \| \| AK_{[1,v]}$
$TK_{[u]}: MAV_{[u,1]} = RAND_{[u,1]} \| CK_{[u,1]} \| IK_{[u,1]} \| \| AK_{[u,1]}, ..., MAV_{[u,v]} = RAND_{[u,v]} \| CK_{[u,v]} \| IK_{[u,v]} \| \| AK_{[u,v]}$
Retrieves the K using KID
Computes SDK and generates ACC_{HSS}
Decrypts the $IMSI$ and ACC_{MS}
Check $ACC_{MS} < ACC_{HSS}$
Verify LAI and MAC_{MS}
Computes MAC_{HSS} and KID_{new}
Generates PAV.
$M_3: (KID_{new} \| SDK \| PAV)$
Computes the MAC_{MME}, $XKSI_{ASME}$ and $AUTH_{MME}$
$M_4: (E(KID_{new})_{SDK} \| AUTH_{MME} \| XKSI_{ASME})$
Retrieves the $RAND_{HSS}$ and TK
Computes the CK, IK, AK and K_{ASME}
Computes the $XMAC_{HSS}$ and $XMAC_{MME}$
Generates $XKSI'_{ASME}$ and computes KSI_{ASME} and RES
$M_5:(RES \| XKSI'_{ASME})$
Computes XRES
Verify $XRES =? RES$
Computes KSI_{ASME}
Message encrypted by K_{ASME}
Acknowledgement of Message
IMSI
KSI_{ASME}
K_{ASME}
.....
IMSI
KSI_{ASME}
K_{ASME}
.....

Fig. 3 Proposed PSE-AKA protocol for LTE/LTE-A networks

To preserve an identity of the objects ($IMSI$), we introduce a new key identifier KID which will be uniquely assigned to K of MS and HSS. The KID is used to generate a new secret dynamic key (SDK) as follows:

$$SDK = f_1'(KID)_K \tag{1}$$

Step-1: The MS transmits an attach request to the MME with its $IMSI$, newly generated accumulator ACC_{MS}, KID and message authentication code (MAC_{MS}). The parameters $IMSI$ and ACC_{MS} are encrypted using secret dynamic key (SDK). The MAC_{MS} is computed as $MAC_{MS} = f_2(IMSI||ACC_{MS}||LAI)_K$.

Step-2: Before offering the services to the MS, a set of MAVs are computed by the MME in advance as follows:

- Total 'u' sets of temporary key $TK[i]$ (for $i = 1$ to u) are randomly generated bythe MME and 'v' sets of $MAV[i, j]$ (for $j = 1$ to v) are generated as $MAV[u, v] = RAND[u, v]|| CK[u, v]||IK[u, v]||AK[u, v]$ for each $TK[u]$. Here $RAND[u, v]$ is a random number. Overall, ($u * v$) vectors are generated from $\{TK[u], MAV[u, v]\}$.

$$CK[u, v] = f_4(RAND[u, v])_{TK[u]} \tag{2}$$

$$IK[u, v] = f_5(RAND[u, v])_{TK[u]} \tag{3}$$

$$AK[u, v] = f_6(RAND[u, v])_{TK[u]} \tag{4}$$

- The MME also computes the session key K_{ASME} (Key for Access Security Management Entity) as $K_{ASME}[u, v] = KDF(CK[u, v]||IK[u, v]||AK[u, v])_{TK[u]}$
- These computations at MME are carried out in advance and can be reused in future. To defeat the replay attack in phase-2, the condition $RAND[i, k] > RAND[i, k-1]$ (for $k = 1$ to n) must be true.

Step-3: After receiving $(IMSI||ACC_{MS})_{SDK}||KID||MAC_{MS})$ from the MS, the MME randomly picks one tuple, called i^{th} tuple from computed MAVs and selects TK in that tuple. Finally, TK is transferred with the LAI to the HSS.

Step-4: After receiving the authentication parameters relayed from MME, HSS executes the following:

- Using the KID, the HSS retrieves the respective key (K) and computes the SDK as shown in Eq 1.
- Then, HSS decrypts the $E(IMSI||ACC_{MS})_{SDK}$ that provides access to the $IMSI$ and ACC_{MS}.
- HSS compares the ACC_{MS} and ACC_{HSS} counted by the HSS. The HSS considers it as a replay attack if $ACC_{MS} < ACC_{HSS}$.
- HSS compares the received value of $IMSI$ with the stored one at the HSS. If it holds, the $IMSI$ is validated. Otherwise, an authentication failure message is transmitted to the MS.
- After retrieving the $IMSI$ and K, HSS computes the MAC'_{MS} using K and verifies whether computed MAC'_{MS} matches with the received MAC_{MS} or not. If it holds, the MS is authenticated by the HSS otherwise; an authentication failure message is transmitted to the MS.
- HSS verifies the LAI received from the MME and matches with the MS's LAI. If they match, HSS authenticates the LAI. Otherwise, HSS declines the authentication request of the MME.

Step-5 After successful verification of MAC_{MS} and LAI, HSS generates the authentication response message as

- HSS generates the $MAC_{HSS} = f_2(ACC_{HSS}||TK||AMF)_K$.
- Finally, the HSS generates the prescriptive authentication vector (PAV) as $PAV = (MAC_{HSS}||ACC_{HSS}||AMF)$.
- For the initial session, a unique KID is assigned to the K by the operator. For subsequent sessions, the HSS assigns a new (KID_{new}) to the K and transmits the $(KID_{new}||SDK||PAV)$ to the MME.

3.3 Phase-2: authentication and key agreement phase

If the MS has registered at phase-1, MS can execute phase-2 for 'n' connections. In phase-2, the MS and MME authenticate to each other and generate several encryption keys. A short description of phase-2 is as follows.

Step-6: After acquiring $(KID_{new}||SDK||PAV)$ from the HSS, MME stores the IMSI (by decrypting the message from MS using SDK) and retrieves the MAC_{HSS} from PAV.

Step-7: The next unused MAV's for $TK[i]$ in i^{th} tuple, called $MAV[i, j]$ is selected by the MME. RAND[i,j] is retrieved from $MAV[i, j]$ by the MME, further called as $RAND_{MME}$. The MME also selects the respective $K_{ASME}[i, j]$, further it is consider as K_{ASME}.

Step-8: MME generates the $XKSI_{ASME}$ and computes the $MAC_{MME} = f_2(MAC_{HSS}||RAND_{MME}||XKSI_{ASME}||AMF)_{K_{ASME}}$ and generates its authentication token as $AUTH_{MME} = (MAC_{MME}||RAND_{MME}||TK||MAC_{HSS}||ACC_{HSS}||AMF)$.

Step-9: After computing the authentication token, MME transmits $AUTH_{MME}$ to the MS concatenating with $XKSI_{ASME}$ and newly generated KID_{new} encrypted under SDK by encryption function E i.e. $(AUTH_{MME}||XKSI_{ASME}||E(KID_{new})_{SDK})$.

Step-10: After acquiring $AUTH_{MME}$ from the MME, the MS performs the following steps:

- The MS computes the CK, IK and AK as shown in Eqs. 2, 3 and 4 respectively. The MS generates the $K_{ASME} = KDF(CK||IK||AK)_{TK}$.
- The MS computes the $XMAC_{HSS} = f_2(ACC_{HSS}||TK||AMF)_K$ and compares it with the received MAC_{HSS}. If they match, the HSS is authenticated by the MS. Otherwise, MS terminates the authentication process.
- The MS computes the $XMAC_{MME} = f_2(XMAC_{HSS}||RAND_{MME}||XKSI_{ASME}||AMF)_{K_{ASME}}$ and verifies with the MAC_{MME}. If they match, the MME and HSS are authenticated by the MS. Otherwise, MS terminates the connection.
- MS generates the $XKSI'_{ASME}$ and computes the KSI_{ASME} by using received $XKSI_{ASME}$ and generated $XKSI'_{ASME}$ as inputs to a predefined $f'()$ function shared between the MME and the MS.
- Then, the MS computes the signed response value RES as $RES = f_3(RAND_{MME}||XKSI'_{ASME})_{K_{ASME}}$ and transmits to the MME along with $XKSI'_{ASME}$.

Step-11: After receiving RES from the MS, MME computes the $XRES = f_3(RAND_{MME}||XKSI'_{ASME})_{K_{ASME}}$ and compares it with the received RES. If both are equal, the MS is verified by the MME and the MME generates a new KSI_{ASME} by putting $XKSI_{ASME}$ and $XKSI'_{ASME}$ to the $f'()$.

Hence, the MS and MME have the same KSI_{ASME} without transmitting it over the network.

Step-12: The MS and MME store K_{ASME} and KSI_{ASME} in their database. After completing the authentication process, the MME sends an encrypted message to the MS, and finally, MS acknowledges the receipt of message to the MME.

The objective of the proposed PSE-AKA protocol is to resolve the security issues of the existing protocols, including the problem of high computational overhead and bandwidth utilization in the communication network. In the existing protocols, all the AV's are generated by the HSS and transmitted to the MME that generates the problem of high computation and bandwidth utilization in the network. In the proposed PSE-AKA protocol, the HSS needs to generate only one set of AVs in place of n set of AVs. The result is improved than the existing protocols and minimizes the inherent problem of high computation overhead at the HSS. However, the computational overhead increases at MME in the proposed protocol. Although, these computations can be reused in the authentication process. Therefore, it will not increase the computational delay during the authentication process. In the proposed protocol, once the registered MME receives the authorization from the HSS, the validity period of this legitimate connection is set by the HSS. Whenever the network is busy, the HSS can authorize the MME to extend authentication time. Hence, the DoS attack can be avoided from the network.

4 Formal verification and simulation of the proposed protocol

The authenticity of the proposed PSE-AKA protocol is analyzed using the BAN logic model and AVISPA tool. The BAN logic formally verifies the correctness of the cryptographic protocols. Moreover, the protocol is simulated by the AVISPA tool and illustrates the security against various known attacks. The analysis shows that the protocol fulfills all the security goals and is free from the malicious attacks.

4.1 Formal verification of the proposed PSE-AKA protocol

In this section, we formally demonstrate the authentication process of the proposed PSE-AKA protocol using the BAN-Logic. The BAN logic is defined by Burrows, Abadi and Needham to formalize the description and analysis of the authentication protocols [43]. The BAN logic is a methodology of logical verification of authentication protocol which formally states the knowledge of information. It formally verifies the information exchanged and the trust among communication entities at each step in the AKA protocols [43–46]. For the formal analysis of the proposed protocol, following assumptions can be considered such as P and Q are the principals; K is the encryption key; K_p and K_q are the public keys, $K_{p^{-1}}$, and $K_{q^{-1}}$ are the corresponding secret keys; X and Y are the statements; K_{ab}, K_{as}, K_{bs} are the shared secret keys and N_a, N_b are the specific statements. The basic symbols and notations of the BAN logic model with their definitions are shown in the Table 3.

The conventional/formal messages in the proposed protocol

- M_1: $MS \rightarrow MME$: $(IMSI, Na)_{SDK}, KID, MAC_1$
- M_2: $MME \rightarrow HSS$: $(IMSI, Na)_{SDK}, KID, MAC_1, LAI, TK$
- M_3: $HSS \rightarrow MME$: $KID, SDK, PAV = (MAC_2, Nb, AMF)$
- M_4: $MME \rightarrow MS$: $(KID)_{SDK}, AUTH_{MME} = (MAC_3, Nc, TK, MAC_2, Nb, AMF), XKSI_{ASME}$
- M_5: $MS \rightarrow MME$: $RES, XKSI'_{ASME}$

4.1.1 Transform messages into idealized logical form

- M_1: $MS \rightarrow MME$: $(Na)_{f_1'(KID)_k}, f_2(Na, LAI)_k, MS \overset{K}{\leftrightarrow} HSS, MS \overset{KID}{\Longleftrightarrow} HSS$
- M_2: $MME \rightarrow HSS$: $(Na)_{f_1'(KID)_k}, f_2(Na, LAI)_k, LAI, MME \overset{TK}{\Leftrightarrow} HSS$
- M_3: $HSS \rightarrow MME$: $Nb, f_2(Nb, TK, LAI)_k, MS \overset{SDK}{\longleftrightarrow} HSS, HSS \overset{K}{\leftrightarrow} MS$
- M_4: $MME \rightarrow MS$: $(KID)_{f_1'(KID)_k}, Nc, TK, f_2(MAC_2, Nc, XKSI_{ASME}, AMF)_X, f_2(Nb, TK, LAI)_k, Nb$
  where, $X{=}KDF(f_4(Nc)_{TK}, f_5(Nc)_{TK} f_6(Nc)_{TK})_{TK}$
- M_5: $MS \rightarrow MME$: $f_3(Nc, XKSI'_{ASME})_X, XKSI'_{ASME}$
  where $X{=}KDF(f_4(Nc)_{TK}, f_5(Nc)_{TK}, f_6(Nc)_{TK})_{TK}$

Table 3 BAN logic notations and their definition

Notation	Definition
$P\mid\equiv X$	P believes X : P believes that X is true
$P\mid\sim X$	P once said X : At some time, P sends a message including statement X
$P \triangleleft X$	P sees X : P reads and receives the message X
$P\mid\Rightarrow X$	P has jurisdiction over X : P has an authority over X and should be trusted
$\#(X)$	X has not sent the message at any time before execution the protocol
$\{X\}_Y$	X is associated with Y and Y is secret
$\xrightarrow{k}$P	P has K as a public key
$P \overset{\text{K}}{\leftrightarrow} Q$	P and Q has shared secret key K
$P \overset{\text{X}}{\Leftrightarrow} Q$	Only P and Q know the secret formula X

4.1.2 Security assumptions

The following assumptions are considered to analyze the protocol.

- A_1: It is considered that the key K is shared between MS and HSS.
  1. $MS| \equiv MS| \overset{\text{K}}{\leftrightarrow} HSS$
  2. $HSS| \equiv MS| \overset{\text{K}}{\leftrightarrow} HSS$
- A_2: It is considered that the channel between MME and HSS is safe.
  1. $MME| \equiv MME| \overset{\text{S}}{\leftrightarrow} HSS$
  2. $HSS| \equiv MME| \overset{\text{S}}{\leftrightarrow} HSS$

     where; *S* is the conveyance message between MME and HSS.
- A_3: It is considered that the MME trusts the HSS.
  1. $MME| \equiv HSS| \Rightarrow MS \overset{\text{K}}{\leftrightarrow} HSS$, MME believes that HSS has a control over shared secret key K between MS and HSS.
  2. $\frac{MME|\sim P, HSS \triangleleft P}{HSS|\equiv MME|\equiv P}$, MME once said principle P, as MME sent P it is known that the MME believes P also HSS sees P, implies that HSS believes MME believes P.
  3. $\frac{HSS|\sim P, MME \triangleleft P}{MME|\equiv HSS|\equiv P}$, HSS once said principle P, as HSS sent P it is known that the HSS believes P also MME sees P, implies that MME believes HSS believes P.
- A_4: It is considered that the KID is shared secret between MS and HSS.
  1. $MS| \equiv MS| \overset{\text{KID}}{\Longleftrightarrow} HSS$
  2. $HSS| \equiv MS| \overset{\text{KID}}{\Longleftrightarrow} HSS$
- A_5: It is considered that the SDK is shared secret key between MS and HSS.
  1. $MS| \equiv MS| \overset{\text{SDK}}{\longleftrightarrow} HSS$
  2. $HSS| \equiv MS| \overset{\text{SDK}}{\longleftrightarrow} HSS$

4.1.3 Annotated statement of protocol analysis

- M_1: $MS \rightarrow MME : MS \mid\equiv \#(Na) \wedge MME \mid\equiv \#(Na)$; $MME \triangleleft (Na)_{f_1'(KID)_k}, f_2(Na, LAI)_k$
- M_2: $MME \rightarrow HSS$: $HSS \mid\equiv \#(Na) \wedge HSS \mid\equiv \#(Nb)$, $HSS \triangleleft (Na)_{f_1'(KID)_k}, f_2(Na, LAI)_k$ after receiving verify $f_2(Na, LAI)_k$
- M_3: $HSS \rightarrow MME$: $HSS \mid\equiv \#(Nb) \wedge MME \mid\equiv \#(Nc)$, $MME \triangleleft f_1'(KID)_k, Nb, f_2(Nb, TK, LAI)_k$
- M_4: $MME \rightarrow MS$: $MME \mid\equiv \#(Nc) \wedge MS \mid\equiv \#(Na)$, $MS \triangleleft (KID)_{f_1'(KID)_k}, Nc, TK, f_2(Nb, TK, LAI)_k, Nb, f_2(MAC_2, Nc, XKSI_{ASME}, AMF)_X$ where, $X = KDF(f_4(Nc)_{TK}, f_5(Nc)_{TK}, f_6(Nc)_{TK})_{TK}$
- M_5: $MS \rightarrow MME$: $MS \mid\equiv \#(Na) \wedge$ MME $\mid\equiv \#(Nc)$, $MME \triangleleft f_3(Nc, XKSI'_{ASME})_X, XKSI'_{ASME}$ where, $X{=}KDF(f_4(Nc)_{TK}, f_5(Nc)_{TK}, f_6(Nc)_{TK})_{TK}$

4.1.4 Inference rules of BAN logic

The inference rules of BAN logic are as follows.

- (R1) *Message meaning rule:*
  1. $\frac{MS|\equiv(MS \overset{K}{\longleftrightarrow} HSS) \wedge (MS \overset{SDK}{\longleftrightarrow} HSS), HSS \triangleleft f_2(Na,LAI)_k}{HSS|\equiv MS|\sim f_2(Na,LAI)_k}$
  2. $\frac{MME|\equiv KDF(f_4(Nc)_{TK}, f_5(Nc)_{TK}, f_6(Nc)_{TK}) \wedge (MME \overset{K_{ASME}}{\longleftrightarrow} MS) \wedge (MME \overset{SDK}{\longleftrightarrow} MS), MS \triangleleft (KID)_{f_1'(KID)_k}, X, Nc, TK, f_2(Nb,TK,LAI)_k, Nb}{MS|\equiv MME|\sim (KID)_{f_1'(KID)_k}, X, Nc, TK, f_2(Nb,TK,LAI)_k, Nb}$

     Where, $X = f_2(f_2(Nb, TK, LAI)_k, Nc, XKSI_{ASME}, AMF)_{K_{ASME}}$
- (R2) *Jurisdiction rule:*
  1. $\frac{HSS|\equiv MS| \Rightarrow f_2(Na,LAI)_k, HSS|\equiv MS|\equiv f_2(Na,LAI)_k}{HSS|\equiv f_2(Na,LAI)_k}$
  2. $\frac{MME|\equiv HSS| \Rightarrow f_1'(KID)_k, Nb, f_2(Nb,TK,LAI)_k, MME|\equiv HSS|\equiv f_1'(KID)_k, Nb, f_2(Nb,TK,LAI)_k}{MME|\equiv f_1'(KID)_k, Nb, f_2(Nb,TK,LAI)_k}$
  3. $\frac{MS|\equiv MME| \Rightarrow (KID)_{f_1'(KID)_k}, f_2(f_2(Nb,TK,LAI)_k, Nc, XKSI_{ASME}, AMF)_{K_{ASME}}, MS|\equiv MME|\equiv (KID)_{f_1'(KID)_k}, X}{MS|\equiv (KID)_{f_1'(KID)_k}, X}$

     Where, $X = f_2(f_2(Nb, TK, LAI)_k, Nc, XKSI_{ASME}, AMF)_{K_{ASME}}$
- (R3) *Nonce Verification Rule:*
  1. $\frac{MS|\equiv \#(Na) \wedge \#(Nb), MS|\equiv HSS|\sim f_2(Na,LAI)_k}{MS|\equiv HSS|\equiv f_2(Na,LAI)_k}$
  2. $\frac{MME|\equiv \#(Nb) \wedge \#(Nc), MME|\equiv HSS|\sim f_1'(KID)_k, Nb, f_2(Nb,TK,LAI)_k}{MME|\equiv HSS|\equiv f_1'(KID)_k, Nb, f_2(Nb,TK,LAI)_k}$
  3. $\frac{HSS|\equiv \#(Nb) \wedge \#(Nc), HSS|\equiv MME|\sim (KID)_{f_1'(KID)_k}, f_2(f_2(Nb,TK,LAI)_k, Nc, XKSI_{ASME}, AMF)_{K_{ASME}}, Nc, TK, f_2(Nb,TK,LAI)_k, Nb}{HSS|\equiv MME|\equiv (KID)_{f_1'(KID)_k}, f_2(f_2(Nb,TK,LAI)_k, Nc, XKSI_{ASME}, AMF) K_{ASME}, Nc, TK, f_2(Nb,TK,LAI)_k, Nb}$

4.1.5 Protocol goal analysis

- G_1: MS and MME maintains the mutual authentication :

From, Message $M_1, M_2, M_3 \rightarrow MS| \equiv \#(Na) \wedge MME| \equiv \#(Na) \wedge HSS| \equiv \#(Na)$. The mutual authentication between MS and MME/HSS is ensured in the proposed protocol as $MS| \equiv HSS| \equiv MME \wedge MME| \equiv HSS| \equiv MS \rightarrow MS| \equiv MME \wedge MME| \equiv MS$.

- G_2: Key compliance achieved among communication entities:

  There is K_{ASME} between the MME and MS to provide the key agreement. $MS| \equiv \#(N_a)$; and $MS| \equiv K_{ASME} \wedge \#(N_c)$. $MS| \equiv k$, $MS| \equiv CK = f_4(Nc)_{TK} \wedge IK = f_5(Nc)_{TK} \wedge AK = f_6(Nc)$ Since, $K_{ASME} = KDF(f_4(Nc)_{TK}, f_5(Nc)_{TK}, f_6(Nc)_{TK})$.

  In addition, $MS| \equiv HSS| \equiv \#(N_a) \wedge \#(N_b)$; and $MS| \equiv HSS| \equiv SDK$. $MS| \equiv HSS| \equiv K$ Since, $MS| \equiv SDK = f_1'(KID)_K \wedge HSS| \equiv SDK = f_1'(KID)_K$.
- G_3: Key freshness between the MS and MME:

  The key freshness between MS and MME holds as $MS| \equiv MME| \equiv \#(N_a) \wedge \#(N_c) \wedge TK$ and $MS| \equiv HSS| \equiv \#(N_a) \wedge \#(N_b)$ and $MME| \equiv HSS| \equiv \#(N_b) \wedge \#(N_c) \wedge TK$ Since, $CK = f_4(Nc)_{TK} \wedge IK = f_5(Nc)_{TK} \wedge AK = f_6(Nc)$ and $K_{ASME} = KDF(f_4(Nc)_{TK}, f_5(Nc)_{TK}, f_6(Nc)_{TK})$.
- G_4: Confidentiality between the MS and the MME: $\frac{MS|\equiv(MS \overset{K_{ASME}}{\longleftrightarrow} MME), MS \triangleleft f_2(P)_{K_{ASME}}}{MS|\equiv MME|\sim f_2(P)_{K_{ASME}}} \wedge \frac{MME|\equiv(MME \overset{K_{ASME}}{\longleftrightarrow} MS), MME \triangleleft f_3(Nc, XKSI'_{ASME})_{K_{ASME}}}{MME|\equiv MS|\sim f_3(Nc, XKSI'_{ASME})_{K_{ASME}}}$

  Where, $P = MAC_{HSS}, Nc, XKSI_{ASME}, AMF$

The formal analysis verifies that the proposed PSE-AKA protocol achieves the mutual authentication among communication entities and protects the confidential information over the communication networks. The protocol resolves various security issues incurred by leakage of IMSI, LAI, and KSI_{ASME} that increases the security of session key. Furthermore, the detailed security analysis of the proposed protocol is illustrated in Section 5.

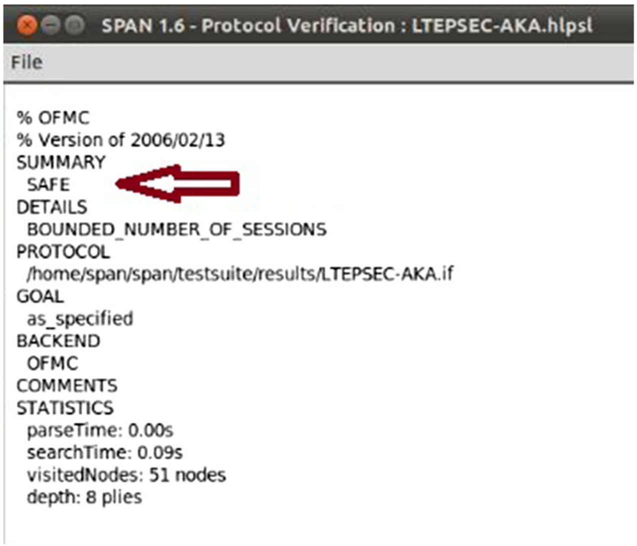
4.2 Proposed protocol simulation using AVISPA tool

In this subsection, simulation of the proposed protocol is carried out using AVISPA tool. The simulation result proves the correctness of the protocol and validates the data integrity, confidentiality, and key secrecy properties. AVISPA supports various security analysis and verification models such as SATMC (SAT-based Model-Checker), OFMC (On-the-Fly-Model-checker) and Cl-AtSe (Constraint Logic-Based Attack Searcher) [47–49]. The main objectives of the protocol are to provide the mutual authentication and achieve the secrecy of pre-shared symmetric keys between the communication entities. The goals of the protocol are shown in Fig. 4.

In the proposed protocol, there are three participants such as MS, MME, and HSS. The protocol is coded in High Level Protocol Specifications Language (HLPSL) to verify security properties of the protocol [50, 51]. The basic role of these participants is described in HLPSL code. We verify the proposed protocol using using OFMC and CL-AtSe

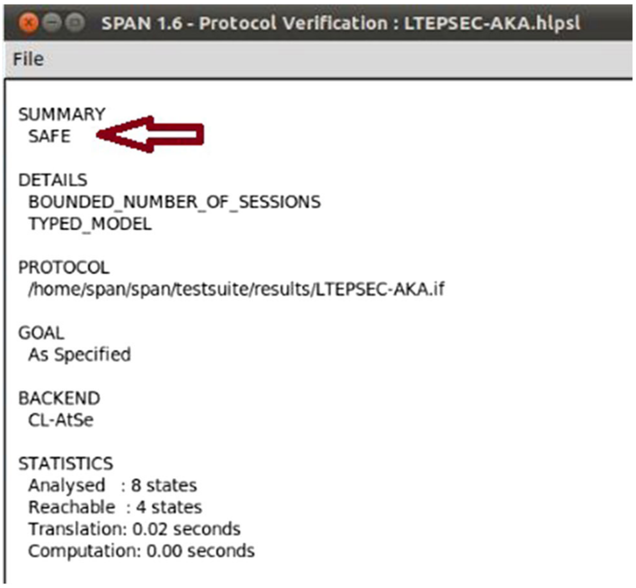
```
goal
secrecy_of sec_skey, sec_tkey
authentication_on mobile_hss
authentication_on mobile_mme
authentication_on hss_mme
end goal
```

Fig. 4 Goals of the proposed protocol



```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/LTEPSEC-AKA.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.09s
  visitedNodes: 51 nodes
  depth: 8 plies
```

Fig. 5 Simulation result of OFMC backend



```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/LTEPSEC-AKA.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS
  Analysed   : 8 states
  Reachable  : 4 states
  Translation: 0.02 seconds
  Computation: 0.00 seconds
```

Fig. 6 Simulation result of CL-AtSe backend

model checker and the results are shown in the Figs. 5 and 6. The SAFE keyword in Figs. 5 and 6 prove that the protocol achieves the specified goals and avoids all the identified attacks.

5 Security analysis of the proposed PSE-AKA protocol

The proposed protocol follows the architecture of EPS-AKA protocol designed by the 3GPP. Hence, the protocol suffers from similar security issues as EPS-AKA protocol. In this section, we analyze the security of the proposed protocol in terms of the security goals, security properties and resistance against various attacks.

- ***Mutual authentication and key compliance***: The Goal G_1 and G_2 (in Section 4.1) of the proposed protocol proves that the MS and MME establish the mutual authentication. In addition, HSS transfers the $PAV = (MAC_{HSS}||ACC_{HSS}||AMF)$ to the MME. MME also transfers the $AUTH_{MME}$ to the MS that contains the MAC_{HSS} and MAC_{MME}. Then, MS generates the $XMAC_{HSS}$ and $XMAC_{MME}$ and MS authenticates the MME and HSS. After this, MS sends the response message $RES = f_3(RAND_{MME}||XKSI'_{ASME})_{K_{ASME}}$ to the MME. MME computes the $XRES$ and verifies the MS. HSS also verifies the MS on behalf of the MME. Hence, the protocol maintains the mutual authentication between the communication entities.
- ***Privacy preservation***: To maintain the privacy of the MS/object in the proposed protocol, MS generates the SDK. The SDK is computed by the KID and pre-shared cryptographic function f'_1. The identity of the MS is encrypted by respective SDK and MS transfers $(E(IMSI||ACC_{MS})_{SDK}||KID||MAC_{MS})$ in a secure network. Moreover, a unique SDK and KID is used at each connection of MS. Hence, an adversary can't achieve the legitimate identity of the MS.
- ***Protection from single key exposure problem***: To protect the shared secret key, the proposed protocol uses the one-way shared secret crypto function (f'_1). The dynamic key SDK is derived from the K (as shown in Eq. 1) using the function f'_1. An adversary never computes the SDK as one has to know f'_1 and the KID. Moreover, the f'_1 is irreversible one-way function so even if the adversary finds out the SDK and f'_1, he/she cannot retrieve the K. Hence, the proposed protocol avoids the single key exposure problem during the authentication process.
- ***Key forward/backward secrecy***: In the proposed protocol, for each fresh authentication request, the MS and MME generate a fresh SDK, K_{ASME}, and the other derived keys. Hence, it is merely impossible for an adversary to retrieve any information based on the link-ability among the various requests. Moreover, an adversary cannot use the keys in the previous session as the communication entities compute the new session keys and derived keys in each session.
- ***Key theft/Key identity theft attack***: In the proposed protocol, the K_{ASME} is computed using CK and IK at the MME and UE. The SDK and K_{ASME} are never sent over the communication network but are rather generated at the communication entities. Hence, an adversary can never retrieve these keys. Moreover, the KSI_{ASME} identity of the K_{ASME} is transmitted over the network with integrity protection. However, the actual KSI_{ASME} is never transmitted over the communication network, that protects the LTE/LTE-A network from the key id theft attack.
- ***Redirection attack***: In the proposed protocol, the adversary installs a bogus base station to gain the knowledge of the user information. If he/she fails to achieve the user identity, it is impossible for him/her to execute the redirection attack on the communication network. Moreover, an identity of the MS is preserved by SDK. Hence, the adversary will never get the identity of the MS and fails to impersonate them. In addition, the LAI is embedded into MAC_{MS} and sends to the HSS. The HSS compares the embedded LAI with the received one from the MME. The authentication request is discarded if HSS fails to verify the LAI. The proposed protocol protects the user identity and the LAI transmitted over the communication network. Hence, the proposed protocol is free from the redirection attack.
- ***MitM attack***: The privacy preservation of the MS and temporary key (TK) protect the communication network from the MitM attack. In addition, the K_{ASME} is generated between communication entities to prevent the eavesdropping of transmitted messages in the authentication process. MME generates the $XKSI_{ASME}$ and sends the message with it. If adversary tampers the transmitted message and generates the $XKSI_{ASME}$, he/she will never compute the K_{ASME}. Therefore, it is merely impossible for an adversary to generate the legitimate response messages in the communication network.
- ***Replay attack***: In the proposed protocol, the MS computes the MAC_{MS} by using ACC_{MS} and sends to the HSS. HSS also uses the accumulator at its own end (ACC_{HSS}) and sends the verification failure message to the MS if $ACC_{MS} < ACC_{HSS}$. In addition, at each connection request, the unique $RAND_{HSS}$ and $RAND_{MME}$ are used in the authentication process of the protocol. Hence, an adversary can never compute the valid session and temporary keys to perform the replay attack in the proposed protocol.

Table 4 Comparative analysis AKA protocols on the basis of different security properties

Security properties	AKA protocols									
	EPS-AKA [16, 28]	Deng et al. [20]	Koien et al. [25]	Wang et al. [26]	Purkhiabani et al. [17]	Choudhury et al. [31]	Hamandi et al. [23, 33]	Degefa et al. [36]	Saxena et al. [37]	PSE-AKA
SP_1	Sym	Asym	Sym	Asym	Sym	Sym	Hybrid	Sym	Sym	Sym
SP_2	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
SP_3	No	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes
SP_4	No	No	No	No	No	No	No	Yes	Yes	Yes
SP_5	No	No	No	No	Yes	No	No	Yes	Yes	Yes
SP_6	No	No	No	No	No	No	Yes	Yes	Yes	Yes
SP_7	No	No	No	No	No	No	Yes	Yes	Yes	Yes
SP_8	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SP_9	No	No	No	No	No	No	Yes	Yes	Yes	Yes
SP_{10}	No	No	No	No	No	No	Yes	Yes	Yes	Yes
SP_{11}	No	No	No	No	No	No	No	Yes	Yes	Yes
SP_{12}	No	No	No	No	No	No	No	Yes	No	Yes
SP_{13}	No	No	No	No	No	No	No	No	Yes	Yes

Sym: FollowSP_1: Type of cryptosystem; SP_2: Follow the 3GPP standard; SP_3: Privacy preservation and protection; SP_4: KSI_{ASME} protection over the network; SP_5: Network signaling congestion avoidance; SP_6: Protection from redirection attack; SP_7: Protection from MiTM attack; SP_8: Protection from replay attack; SP_9: Protection from impersonation attack; SP_{10}: Protection from DoS attack; SP_{11}: Key forward/backward secrecy; SP_{12}: Avoids the single key problem; SP_{13}: Supports to the IoT based services

- ***Impersonation attack***: Suppose, an adversary computes the MAC'_{MS} by masquerading the identity of MS and sends to the HSS. Also, the HSS computes the MAC_{MS} and compares with received MAC'_{MS}. If the verification fails, a malicious MS is identified by the HSS. In addition, the bogus MS will never generate K_{ASME} and communication between the entities remains secure. Therefore, it is not possible to launch the impersonation attack in the communication network.
- ***DoS attack***: To launch the DoS attack, the adversary can impersonate as the legitimate MS and constantly send the false authentication requests to gain the access of network. In the proposed protocol, MS computes the MAC_{MS} and sends to the HSS. Then, HSS computes the MAC_{MS} and compares it with received one. If the verification fails, HSS identifies the malicious MS in the network and transfers the authentication declined message to the MS. Similarly, MS verifies the authenticity of the HSS by verifying the MAC_{HSS}. If the verification fails, an authentication failure message is transmitted to the MME and HSS. Hence, the proposed protocol resists from the DoS attack during the key operations of the protocol.

The comparative analysis of the different security properties identified for IoT enabled LTE/LTE-A network is shown in Table 4. It can be observed that some of the existing protocols follow the public key cryptosystem to establish vigorous secrecy and confidentiality between the communication entities that lead to high computation overhead. Also, these protocols do not follow the basic architecture of the LTE network defined by 3GPP committee. It is observed that the existing AKA protocols fail to fulfill all the security goals and suffers from the single key problem during the AKA process. Different from existing AKA protocols, the proposed protocol follows the symmetric key cryptography to generate the authentication vectors in the AKA process. Also, the protocol follows the standards of the 3GPP committee and mandates the privacy preservation of each device in the communication network. In addition, the proposed protocol solves the single key exposure problem from the communication network. Moreover, the protocol defeats all the identified attacks and realizes the KFS/KBS efficiently. Hence, the proposed PSE-AKA protocol is comparatively superior to the existing AKA protocols in the LTE/LTE-A networks.

6 Performance evaluation of the proposed PSE-AKA protocol

In this section, we evaluate the performance of the proposed PSE-AKA protocol in terms of communication overhead, computation overhead, storage overhead, and network bandwidth utilization. To evaluate the performance on the basis of computation overhead of the AKA protocols, the standard elapsed time of the cryptographic functions is tested in multi-precision integer and rational arithmetic library (MIRACL) C/C++ library and adopted the simulation environment at Pentium Core 2 Duo processor which consists of 4 GB RAM and 3 GHz speed [52, 53]. We assumed that both the mobile user and HSS have same computing power despite the difference between two computing machines. We consider each function as a unit value and on the basis of the number of function executed by the protocol, the computation overhead is computed. The analysis shows that the proposed protocol achieves the desired goals of the IoT enabled LTE/LTE-A network efficiently.

6.1 Communication overhead

To achieve the mutual authentication among communication entities, various messages are transmitted over the communication network. We compute the transmitted message size to evaluate the communication overhead of the proposed PSE-AKA and existing protocols in LTE/LTE-A network.

Table 5 Communication overhead of the AKA protocols in LTE/LTE-A networks

AKA protocols	Communication overhead per message							
	M1	M2	M3	M4	M5	M6	M7	Total
EPS-AKA Protocol [16, 28]	192	323	448	288	419	64	–	1734 bits
Deng et al. Protocol [20]	384	512	736	387	64	–	–	2083 bits
Koien's et al. Protocol [25]	260	436	608	288	128	112	48	1880 bits
Wang et al. Protocol [26]	256	384	704	387	64	–	–	1795 bits
Purkhiabani et al. Protocol [17]	384	643	608	419	64	–	–	2118 bits
Choudhury et al. Protocol [31]	166	174	922	436	64	128	–	1890 bits
Hamandi et al. Protocol [33]	128	256	992	256	64	–	–	1696 bits
Degefa et al. Protocol [36]	448	448	640	432	64	–	–	2032 bits
Saxena et al. Protocol [37]	320	515	432	179	67	134	–	1647 bits
PSE-AKA Protocol	320	488	392	587	67	–	–	1854 bits

All the protocols are assumed to be of standard sizes with respect to various parameters as shown in the Table 1. To compute the communication overhead, we consider the single authentication vector is being transmitted from the HSS to MME. The total number of bits in the messages transmitted by the AKA protocols of LTE/LTE-A network are shown in Table 5. Table 5 shows that the communication overhead of the proposed protocol is less compared to the existing AKA protocols. However, the EPS-AKA protocol generates the minimum overhead compared to PSE-AKA but, it suffers from the privacy preservation problem and several network attacks. Also, the Wang's and Hamandi's protocol has the minimum communication overhead but, these protocols follow the public key cryptosystem that leads to high computation overhead. Moreover, the communication overhead generated by the Saxena et al. is less compared to proposed protocol but, the protocol does not consider the single key exposure problem and generates the high computation at HSS.

The total communication overhead generated by the proposed PSE-AKA protocol during authentication is ((1854/1734)*100 = 106.90%), 89.00%, 98.61%, 103.28%, 87.53%, 98.09%, 109.31%, 91.24% and 112.50% of the EPS-AKA, Deng et al., Koien's et al., Wang et al., Purkhiabani et al., Choudhury et al., Hamandi et al., Degefa et al. and Saxena et al. protocols respectively. Hence, the proposed protocol reduces the total communication overhead during authentication process by 11%, 1.39% , 12.47%, 1.91%, 8.76% compared to Deng et al., Koien's et al., Purkhiabani et al., Choudhury et al., and Degefa et al. respectively. However, the protocol utilizes the -6.90%, -3.28%, -9.31% and -12.50% more overhead compared to the EPS-AKA, Wang et al., Hamandi et al. and Saxena et al. protocols respectively. Different from these protocols, the proposed protocol fulfills all the security requirements of the IoT enabled LTE/LTE-A network with competitive communication overhead.

6.2 Computation overhead

In this section, the proposed PSE-AKA protocol is compared with existing protocols in terms of computation overhead. The variety of functions shown in Table 2 are used to generate the different parameters in the authentication process. The computation overhead of each protocol is evaluated on the basis of these functions. To maintain the consistency while evaluating the computation overhead, all the computation functions are considered unit value. We evaluate the total computation overhead of each protocol as shown in Table 6. Koien's protocol generates the minimum computation overhead because the K_{ASME} is not generated using standard keys and an adversary can easily compromise the security of K_{ASME}. In addition, Fig. 7 illustrates the

Table 6 Computation overhead of the AKA protocols in LTE/LTE-A networks

Communication entities	AKA Protocols									
	EPS-AKA [16, 28]	Deng et al. [20]	Koien's et al. [25]	Wang et al. [26]	Purkhiabani et al. [17]	Choudhury et al. [31]	Hamandi et al. [33]	Degefa et al. [36]	Saxena et al. [37]	PSE-AKA
No. of functions at MS	05	08	05	08	12	06	08	08	10	10
No. of functions at MME	03	02	01	03	05	04	04	02	03	07
No. of functions at HSS	05	07	05	07	06	05	07	07	07	04
Total No. of functions	13	17	11	18	23	15	19	17	20	21

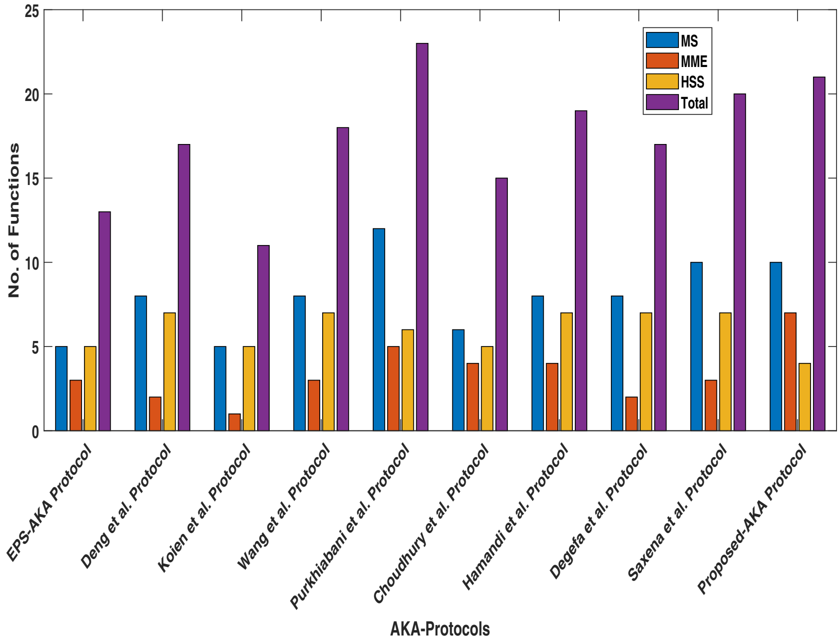


Fig. 7 Comparative analysis of the computation overhead

comparative study of the computation overhead incurs in the several AKA protocols of the LTE/LTE-A network. It is observed that the computational consumption of the existing AKA protocol is very much competitive with the proposed PSE-AKA protocol. But, the existing protocols do not preserve the privacy of user identity and are susceptible to various attacks over the network. Different from existing AKA protocols, the keys are never transmitted over the communication network in the proposed protocol. Also, the proposed protocol achieves the key secrecy and maintains the KFS/KBS. Moreover, the protocol resolves the single key exposure problem, preserves the privacy of user identity, protects the KSI_{ASME} and avoids all the possible attacks from the communication network.

6.3 Bandwidth utilization

The proposed PSE-AKA protocol follows the cocktail therapy to generate the authentication vectors in the authentication process. The proposed scheme shares the vector generation load among the communication entities. In the PSE-AKA protocol, HSS generates a PAV and sends to the MME. When the authentication process is initiated, the MME dispenses the MAV and PAV to generate the effective AVs for mutual authentication. The proposed PSE-AKA protocol reduces the bandwidth utilization between the communication entities and computational overhead from the HSS. From Table 7, it is observed that the protocol minimizes the bandwidth utilization by (100-(880/963)*100 =) 8.62%, 29.49%, 26.92%, 19.12%, 18.14%, 19.71%, 29.41%, 19.12% and 7.37% compared to the EPS-AKA, Deng et al., Koien's et al., Wang et al., Purkhiabani et al., Choudhury et al., Hamandi et al., Degefa et al. and Saxena et al. protocols respectively. In addition, the comparative analysis of the bandwidth utilization of the proposed PSE-AKA and the existing AKA protocols is graphically shown in the Fig. 8. The bandwidth utilization between the UE and MME is slightly higher as compared to the existing protocols for a single authentication. However, different from these protocols, the proposed protocol overcomes the problem of single key exposure, privacy preservation and avoids the attacks from the LTE/LTE-A network.

Table 7 Bandwidth consumption of the AKA protocols in LTE/LTE-A networks

Bandwidth utilization	AKA protocols									
	EPS-AKA [16, 28]	Deng et al. [20]	Koien's et al. [25]	Wang et al. et al. [26]	Purkhiabani et al. [17]	Choudhury [31]	Hamandi et al. [33]	Degefa et al. [36]	Saxena et al. [37]	PSE-AKA
Between MS and MME	771	835	676	707	944	794	448	944	697	974
Between MME and HSS	963	1248	1204	1088	1075	1096	1248	1088	950	880

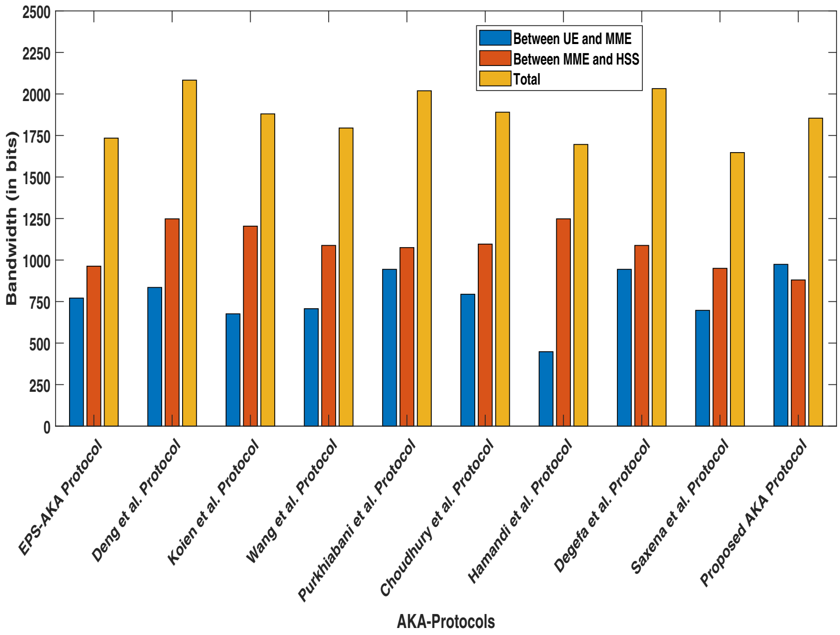


Fig. 8 Comparative analysis of the bandwidth utilization

6.4 Storage overhead

In this subsection, we analyze the storage overhead of different AKA protocols at MME of the communication networks. All the AKA protocols need to store authentication vector generated by the HSS on MME for further authentication process. In the proposed PSE-AKA protocol, the MME combines its MAV with the PAV produced by the HSS to compute the adequate AVs used for mutual authentication. In the proposed scheme, the MME retains MAVs to generate the AVs. However, these MAVs can be reused without increasing the overhead at the MME. So, different from the existing AKA protocols, the MME needs to store only one PAV instead of n-sets of AVs during the authentication process. The comparative study of the storage overhead with respect to various AKA protocols is shown in Table 8. It clearly shows that the proposed PSE-AKA protocol reduces the storage overhead of the MME compared to the existing AKA protocols of the LTE/LTE-A network.

Table 8 Comparison of storage overhead at MME

AKA protocols	Storage Overhead (bits)
EPS-AKA [16, 28]	$448n$
Deng et al. [20]	$736n$
Koien's et al. [25]	$608n$
Wang et al. [26]	$704n$
Purkhiabani et al. [17]	$608n$
Choudhury et al. [31]	$922n$
Hamandi et al. [33]	$992n$
Degefa et al. Protocol [36]	$640n$
Saxena et al. [37]	$432n$
PSE-AKA	$392n$

7 Conclusion

In this paper, the performance and security enhanced cocktail-AKA protocol is proposed for IoT enabled LTE/LTE-A networks. The cocktail therapy is used to generate the authentication parameters that reduces the computation overhead and bandwidth utilization between the HSS and MME. The protocol improves the authentication process and provides an environment that enables secure communications among IoT objects in the networks. Moreover, the protocol avoids the single key exposure problem, preserves the privacy of user identity, protects the KSI_{ASME} and avoids all the possible attacks from the communication network. The correctness of the proposed protocol is formally verified using BAN logic. The protocol is also simulated using AVISPA tool that shows the protocol achieves all the security goals. The security analysis shows that the proposed protocol avoids the security attacks from the communication networks. Further, the performance analysis shows that the proposed PSE-AKA protocol generates the minimum communication overhead, computation overhead and storage overhead compared to the existing AKA protocols. In addition, the protocol has significant improvement in the bandwidth utilization between HSS and MME. To the best of our knowledge, it is the first attempt to preserve the privacy of communication entities and avoid the single key exposure problem from the communication network. Therefore, it is expected that the proposed protocol will strengthen the performance and security of the IoT enabled LTE/LTE-A network.

In the group based AKA protocols, a long delay and high overhead will be generated whenever the mass devices/objects simultaneously request for the authentication. In addition, the AKA process suffers from the signaling congestion and various security attacks. Therefore, the proposed protocol can be explored for group-based communication in the LTE/LTE-A network.

Appendix : HLPSL code defining the role of MS, MME and HSS

Role1: Mobile Station

```
role mobile(M, V, H:agent,
            SND, RCV: channel(dy),
            SKey1, TKey1: symmetric_key,
            Imsi, Guti,Kid, ACCms, ACCmme, ACChss,
            Amf:text,
            E1,F1,F2,F3,F4,F5,F6,KDF:function)
played_by M
def=
  local
    State :nat,
    XKSIasme, LAI, Rmme, Rms, Rhss:text
    const  sec_skey, sec_tkey, mobile_mme, hss_mme,
    mobile_hss : protocol_id,
    success     : text
  init  State := 0
  transition
 1.  State = 0 /\ RCV(start) =|>
     State’:= 1
               /\ SND (E1(F1(SKey1.Kid).Imsi.ACCms).
                  Kid.F2(SKey1.Imsi.ACCms.LAI))
               /\ secret(Imsi,Kid, sec_skey,{M,H,V})
               /\ witness(M,V, mobile_mme,ACCms)
               /\ request(M,H,V, mobile_hss,ACCms)
 2. State = 1 /\ RCV (E1(F1(SKey1.Kid)).Kid.XKSIasme
                 .(F2(KDF(TKey1.F4(TKey1.Rmme’)
                 .F5(TKey1.Rmme’).F6(TKey1.Rmme’))
                 .F2(SKey1.ACChss.TKey1.Amf).Rmme’.
                  XKSIasme.ACCmme.Amf))
                 .Rmme’.TKey1.F2(SKey1.ACChss.TKey1
                 .Amf).ACChss.Amf) =|>
   State’:= 2  /\ XKSIasme’ := new()
               /\ SND (F3(KDF(TKey1.F4(TKey1.Rmme’)
                 .F5(TKey1.Rmme’).F6(TKey1.Rmme’)))
                 .Rmme’.XKSIasme’)
               /\ secret(Imsi, sec_tkey,{M,H,V})
               /\ witness(M,H, mobile_mme,XKSIasme’)
               /\ request(M,H,V, mobile_mme,Rmme’)
 3. State   = 2 /\ RCV (Guti.E1(KDF(TKey1.F4(TKey1
                  .Rmme’).F5(TKey1.Rmme’).F6(TKey1
                  .Rmme’)))) =|>
    State’ := 3
              /\ SND (success)
              /\ request(M,H,V, mobile_mme,Guti)
 end role
```

Role2: Mobile Management Entity

```
role mme(V, H, M:agent,
         SND, RCV: channel(dy),
         SKey1, TKey1: symmetric_key,
         Imsi, Guti,Kid, ACCms, ACCmme, ACChss,
         Amf:text,
         E1,F1,F2,F3,F4,F5,F6,KDF:function)
played_by V
def=
  local
     State : nat, XKSIasme, LAI, Rmme, Rms, Rhss:text
     const  sec_skey,sec_tkey,mobile_mme,hss_mme,
     mobile_hss : protocol_id,
     success : text
  init State := 0

 transition
 1. State = 0 /\ RCV (E1(F1(SKey1.Kid).Imsi.ACCms)
                 .Kid.F2(SKey1.Imsi.ACCms.LAI)) =|>
  State’:= 1 /\ LAI’ := new()
         /\ SND(E1(F1(SKey1.Kid).Imsi.ACCms).Kid
          .F2(SKey1.Imsi.ACCms.LAI’).Rmme.F4(TKey1
          .Rmme).F5(TKey1.Rmme).F6(TKey1.Rmme))
         /\ secret(Imsi, sec_tkey,{V,H,M})
         /\ witness(V,H, hss_mme, Kid)
         /\ request (V,H,M, mobile_hss, LAI’)
 2. State = 1 /\ RCV (E1(F1(SKey1.Kid).Kid.F2(SKey1
                .ACChss.TKey1.Amf).ACChss.Amf)) =|>
 State’:= 2 /\ Rmme’:=new()
        /\ SND (E1(F1(SKey1.Kid)).Kid.XKSIasme.(F2
         (KDF(TKey1.F4(TKey1.Rmme’).F5(TKey1.Rmme’)
         .F6(TKey1.Rmme’)).F2(SKey1.ACChss.TKey1.Amf)
         .Rmme’.XKSIasme.ACCmme.Amf)).Rmme’.TKey1.
          F2(SKey1.ACChss.TKey1.Amf).ACChss.Amf)
        /\ secret(Imsi,sec_skey,{V,H,M})
        /\ witness(M,H, hss_mme,Rmme’)
        /\ request (V,H,M, mobile_mme, ACChss)
 3. State = 2 /\ RCV(F3(KDF(TKey1.F4(TKey1.Rmme’).F5
               (TKey1.Rmme’).F6(TKey1.Rmme’))).Rmme’
               .XKSIasme’) =|>
 State’ := 3 /\ SND (Guti.E1(KDF(TKey1.F4(TKey1.Rmme’)
                .F5(TKey1.Rmme’).F6(TKey1.Rmme’))))
            /\ secret(Imsi,sec_tkey,{V,H,M})
            /\ witness(M,H, hss_mme,Guti)
            /\ request (V,H,M, mobile_mme, Rmme’)
 4. State = 3 /\ RCV (success) =|>
  State’ := 4
 end role
```

Role3: Home Subscriber Server

```
role hss(H, V, M:agent,
        SND, RCV: channel(dy),
        SKey1, TKey1: symmetric_key,
        Imsi, Guti,Kid, ACCms, ACCmme, ACChss,
        Amf:text,
        E1,F1,F2,F3,F4,F5,F6,KDF:function)
played_by H
def=
  local
      State :nat, XKSIasme, LAI, Rmme, Rms, Rhss:text
      const sec_skey,sec_tkey,mobile_mme,hss_mme,
      mobile_hss: protocol_id,
      success : text
  init  State := 0
  transition
 1. State = 0 /\ RCV(E1(F1(SKey1.Kid).Imsi.ACCms).Kid
               .F2(SKey1.Imsi.ACCms.LAI’).Rmme.F4(TKey1
              .Rmme).F5(TKey1.Rmme).F6(TKey1.Rmme)) =|>
 State’:= 1 /\ SND (E1(F1(SKey1.Kid).Kid.F2(SKey1.
                ACChss.TKey1.Amf).ACChss.Amf))
              /\ secret(Imsi, sec_skey,{H, M,V})
              /\ witness(M,H, mobile_hss, Kid)
              /\ request (V,H,M,  hss_mme, ACChss)
   end role
```

References

1. Jover RP (2015) Security and impact of the IoT on LTE mobile networks. In: Security and Privacy in the Internet of Things (IoT): Models, Algorithms, and Implementations, vol. 6, CRC Press
2. Whitmore A, Agarwal A, Da Xu L (2015) The internet of things a survey of topics and trends. Inf Syst Front 17(2):261–274
3. Kim J, Choi SC, Yun J, Lee J (2018) Towards the oneM2M standards for building IoT ecosystem: analysis, implementation and lessons. Peer-to-Peer Netw Appl 11(1):139–151
4. Ghavimi F, Chen H-H (2015) M2M communications in 3GPP LTE/LTE-a networks: architectures, service requirements, challenges, and applications. IEEE Commun Surv Tutorials 17(2):525–549
5. Kim J, Lee J, Kim J, Yun J (2014) M2M service platforms: survey, issues, and enabling technologies. IEEE Commun Surv Tutorials 16(1):61–76
6. Jang Y, Kim J, Lee W (2017) Development and application of internet of things educational tool based on peer to peer network. Peer-to-Peer Netw Appl 11(6):1217–1229
7. Lin X, Andrews J, Ghosh A, Ratasuk R (2014) An overview of 3GPP device-to-device proximity services. IEEE Commun Mag 52(4):40–48
8. 3rd Generation Partnership Project(3GPP) (2014) Technical specification group services and system aspects; service requirements for machine-type communication (MTC); (release 13), 3GPP TS 22.368 V13.1.0
9. Park RC, Jung H, Chung KY, Kim KJ (2014) Performance analysis of LTE downlink system using relay-based selective transmission. Pers Ubiquit Comput 18(3):543–551
10. Alam M, Yang D, Rodriguez J, Abd-alhameed R (2014) Secure device-to-device communication in LTE-a. IEEE Commun Mag 52(4):66–73
11. Bae WS (2016) Designing and verifying a P2P service security protocol in M2M environment. Peer-to-Peer Netw Appl 9(3):539–545
12. Wang G, Liu T (2018) Resource allocation for M2M-enabled cellular network using Nash bargaining game theory. Peer-to-Peer Netw Appl 11(1):110–123
13. Park Y, Park T (2007) A survey of security threats on 4G networks, Globecom Workshops, 2007. IEEE: 1–6
14. Aiash M, Mapp G, Lasebae A, Phan R (2010) Providing security in 4G systems: unveiling the challenges. In: Sixth advanced international conference on telecommunications (AICT). IEEE, pp 439–444
15. Bikos AN, Sklavos N (2013) LTE/SAE security issues on 4G wireless networks. IEEE Secur Priv 11(2):55–62
16. Abdeljebbar M, Elkouch R (2016) Security analysis of LTE/SAE networks over e-UTRAN. In: International conference on information technology for organizations development (IT4OD). IEEE, pp 1–5
17. Purkhiabani M, Salahi A (2012) Enhanced authentication and key agreement procedure of next generation 3GPP mobile networks. Int J Inform Electronics Eng 2(1):69
18. Vintilă C-E, Patriciu V-V, Bica I (2011) Security analysis of LTE access network. In: Proc. 10th Intl Conf. Networks, pp 29–34
19. Zhang J, Wang ZJ, Quan Z, Yin J, Chen Y, Guo M (2018) Optimizing power consumption of mobile devices for video streaming over 4G LTE networks. Peer-to-Peer Netw Appl 11(5):1101–1114
20. Deng Y, Fu H, Xie X, Zhou J, Zhang Y, Shi J (2009) A novel 3GPP SAE authentication and key agreement protocol. In: IEEE international conference on network infrastructure and digital content (ICNIDC 2009). IEEE, pp 557–561
21. Gu L, Gregory MA (2011) A green and secure authentication for the 4th generation mobile network. In: Australasian telecommunication networks and applications conference (ATNAC 2011). IEEE, pp 1–7
22. Hadiji F, Zarai F, Kamoun L (2009) Authentication protocol in fourth generation wireless networks. In: IFIP International Conference on Wireless and Optical Communications Networks (WOCN 2009). IEEE, pp 1–4
23. Hamandi K, Sarji I, Chehab A, Elhajj IH, Kayssi A (2013) Privacy enhanced and computationally efficient HSK-AKA LTE scheme. In: 27th International conference on advanced information networking and applications workshops (WAINA 2013). IEEE, pp 929–934
24. He D, Wang J, Zheng Y (2008) User authentication scheme based on self certified public-key for next generation wireless network. In: International symposium on biometrics and security technologies (ISBAST 2008). IEEE, pp 1–8
25. Køien GM (2011) Mutual entity authentication for LTE. In: 7th International wireless communications and mobile computing conference (IWCMC 2011). IEEE, pp 689–694
26. Li X, Wang Y (2011) Security enhanced authentication and key agreement protocol for LTE/SAE network. In: 7th International conference on wireless communications, networking and mobile computing (WiCOM 2011). IEEE, pp 1–4
27. Zheng Y, He D, Tang X, Wang H (2005) AKA and authorization scheme for 4G mobile networks based on trusted mobile platform. In: Fifth international conference on information, communications and signal processing. IEEE, pp 976–980
28. Cao J, Ma M, Li H, Zhang Y, Luo Z (2014) A survey on security aspects for LTE and LTE-a networks. IEEE Commun Surv Tutorials 16(1):283–302
29. Peng C, Tu G-H, Li C-Y, Lu S (2012) Can we pay for what we get in 3G data access? In: Proceedings of the 18th annual international conference on mobile computing and networking. ACM, pp 113–124
30. Vintilă C-E, Patriciu V-V, Bica I (2011) A J-PAKE based solution for secure authentication in a 4G network, NEHIPISIC'11 Proceeding of 10th WSEAS international conference on electronics, hardware, wireless and optical communications
31. Choudhury H, Roychoudhury B, Saikia DK (2012) Enhancing user identity privacy in LTE. In: 11th International conference on trust, security and privacy in computing and communications. IEEE, pp 949–957
32. Prasad M, Manoharan R (2015) A robust secure DS-AKA with mutual authentication for LTE-a. Appl Math Sci 9(47):2337–2349
33. Hamandi K, Abdo JB, Elhajj IH, Kayssi A, Chehab A (2017) A privacy-enhanced computationally-efficient and comprehensive LTE-AKA. Comput Commun 98:20–30
34. Ramadan M, Li F, Xu C, Mohamed A, Abdalla H, Ali AA (2016) User-to-user mutual authentication and key agreement scheme for LTE cellular system. IJ Netw Secur 18(4):769–781
35. Baza MI, Fouda MM, Eldien AST, Mansour HA (2015) An efficient distributed approach for key management in microgrids. In: 11th International computer engineering conference (ICENCO-2015). IEEE, pp 19–24
36. Degefa FB, Lee D, Kim J, Choi Y, Won D (2016) Performance and security enhanced authentication and key agreement protocol for SAE/LTE network. Comput Netw 94:145–163
37. Saxena N, Grijalva S, Chaudhari NS (2016) Authentication protocol for an IoT-enabled LTE network. ACM Trans Internet Technol (TOIT) 16(4):25
38. Mohammadali A, Haghighi MS, Tadayon MH, Mohammadi-Nodooshan A (2018) A novel identity-based key establishment method for advanced metering infrastructure in smart grid. IEEE Trans Smart Grid 9(4):2834–2842

39. Sharma C, Vaid R (2019) Analysis of existing protocols in WSN based on key parameters. In: Proceedings of 2nd international conference on communication, computing and networking. Springer, Berlin, pp 165–171
40. Ou H-H, Hwang M-S, Jan J-K (2010) A cocktail protocol with the authentication and key agreement on the umts. J Syst Softw 83(2):316–325
41. Calhoun P, Loughney J, Guttman E, Zorn G, Arkko J (2003) Diameter base protocol, Technical report
42. Fajardo V, Arkko J, Loughney J, Zorn G (2012) Diameter base protocol, Technical report
43. Burrows M, Abadi M, Needham R (1989) A logic of authentication. In: Proceedings of the royal society of london a: mathematical, physical and engineering sciences, vol 426. The Royal Society, pp 233–271
44. Burrows M, Abadi M, Needham R (1988) Authentication: a practical study in belief and action. In: Proceedings of the 2nd conference on theoretical aspects of reasoning about knowledge. Morgan Kaufmann Publishers Inc., pp 325–342
45. Gaarder K, Snekkenes E (1990) On the formal analysis of pkcs authentication protocols. In: Advances in Cryptology AUSCRYPT'90. Springer, pp 105–121
46. Odelu V, Das AK, Goswami A (2015) A secure biometrics-based multiserver authentication protocol using smart cards. IEEE Trans Inform Forensics Secur 10(9):1953–1966
47. Armando A, Basin D, Boichut Y, Chevalier Y, Compagna L, Cuéllar J, Drielsma PH, Héam P-C, Kouchnarenko O, Mantovani J et al (2005) The avispa tool for the automated validation of internet security protocols and applications. In: International conference on computer aided verification. Springer, pp 281–285
48. Avispa Automated Validation of Internet Security Protocols (2003) http://www.avispa-project.org
49. Lai C, Li H, Li X, Cao J (2015) A novel group access authentication and key agreement protocol for machine-type communication. Trans Emerging Telecommun Technol 26(3):414–431
50. Jiang R, Lai C, Luo J, Wang X, Wang H (2013) EAP-based group authentication and key agreement protocol for machine-type communications, Int J Distributed Sensor Netw
51. Lai C, Li H, Lu R, Shen XS (2013) SE-AKA: a secure and efficient group authentication and key agreement protocol for LTE networks. Comput Netw 57(17):3492–3510
52. Michael S Multiprecision integer and rational arithmetic c/c++ library (mir- acl). Available online at https://libraries.docs.miracl.com/miracl-user-manual/installation
53. Gupta M, Chaudhari NS (2019) Anonymous two factor authentication protocol for roaming service in global mobility network with security beyond traditional limit. Ad Hoc Networks 84:56–67

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Balu L. Parne has done his under graduation from Shri Sant Gajanan Maharaj College of Engineering (SSGMCE), Shegaon that is affiliated to Sant Gadge Baba Amravati University (SGBAU), Amravati, Maharashtra, India and post-graduation from National Institute of Technology (NIT), Rourkela, Orissa, India. He submitted his PhD thesis to the Department of Computer Science and Engineering of Visvesvaraya National Institute of Technology (VNIT), Nagpur- 440010, Maharashtra, India. Currently, he is working as the Assistant Professor in the Department of Computer Science and Engineering of Vellore Institute of Technology (VIT-AP) university, Amaravati, Andhra Pradesh. His current area of research is Wireless Communication, Network security, Internet of Things, Mobile computing and its applications.

Shubham Gupta received his B.Tech. in information technology and M.Tech in computer science & engineering from Uttar Pradesh Technical University, Lucknow, and University College of Engineering, RTU, Kota, India respectively. Currently, he is pursuing his Ph.D. in Computer Science & Engineering from Visvesvaraya National Institute of Technology, Nagpur, Maharashtra, India. His research interest includes security in cellular networks, machine type communication, wireless communication networks and mobile computing.

Narendra S. Chaudhari completed his undergraduate, postgraduate and doctoral studies at Indian Institute of Technology (IIT), Mumbai, Maharashtra, India, in 1981, 1983, and 1988 respectively. He has successfully completed 08 R & D Projects funded by DST, UGC, AICTE, MHRD, etc. He has done significant research work on game AI, novel neural network models like binary neural nets and bidirectional nets, graph isomorphism problem, security of the wireless mobile communication, mobile computing and Internet of Things. He has been referee and reviewer for a number of premier conferences and Journals including IEEE Transaction, Neurocomputing, etc. He is fellow and recipient of Eminent Engineer award (Computer Engineering) of the Institution of Engineers, India (IE-India), Bharat Vidya Shiromani Award (with gold medal), as well as fellow of the Institution of Electronics and Telecommunication Engineers (IETE) (India), senior member of Computer Society of India, senior member of IEEE, USA, member of Indian Mathematical Society (IMS), Cryptology Research Society of India (CRSI) and many other professional societies.

Affiliations

Balu L. Parne[1] · **Shubham Gupta**[2] · **Narendra S. Chaudhari**[3]

Shubham Gupta
shubham.gupta@students.vnit.ac.in

Narendra S. Chaudhari
nsc@iiti.ac.in; nsc0183@yahoo.com

[1] Department of Computer Science and Engineering, Vellore Institute of Technology (VIT-AP) University, Amaravati, 522237 Andhra Pradesh, India

[2] Department of Computer Science and Engineering, Visvesvaraya National Institute of Technology (VNIT), Nagpur, 440010 Maharashtra, India

[3] Department of Computer Science and Engineering, Indian Institute of Technology (IIT), Indore, 453552 Madhya Pradesh, India